

7/20/17
UNSEALED PER ORDER OF COURT

SEAL
UNITED STATES DISTRICT COURT

for the
Southern District of California

FILED

APR 22 2016

CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY DEPUTY

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
Facebook Inc, 1601 Willow Road, Menlo Park, CA)
For Records to Facebook User ID:)
<https://facebook.com/profile.php?id=100008589613118>)

Case No.

'16MJ1174

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Northern District of California (identify the person or describe property to be searched and give its location): see Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): see Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 912, and the application is based on these facts: See attached affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of 7 days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Stirling Campbell, HSI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 4/22/16

City and state: San Diego, CA


Judge's signature

Barbara L. Major, United States Magistrate Judge
Printed name and title

1-nbp

NG
76735
04/21/16**AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT**

I, Special Agent Stirling Campbell, upon being duly sworn do hereby state that the following is true to my knowledge and belief:

1. I am a Special Agent with the Department of Homeland Security (DHS), Homeland Security Investigations (HSI) having been so employed since April 2006. I am currently assigned to the Special Agent in Charge (SAC) San Diego Office, Cyber Crimes Group within HSI in San Diego, California. Prior to this time, I worked as a United States Customs and Border Protection Officer in Los Angeles and Long Beach, California for approximately two (2) years and two (2) months. I have a Bachelor's Degree in Economics from the University of California, San Diego. I have received training from the Federal Law Enforcement Training Center in the area of child pornography investigations and pedophile behavior. I have assisted in the service of numerous search warrants involving computer/cyber-crimes. I am currently assigned to the Internet Crimes Against Children (ICAC) task force in San Diego, California. This task force includes members of the San Diego Police Department, San Diego County Sheriff's Department, U.S. Postal Inspection Service, Federal Bureau of Investigations, Naval Criminal Investigative Service, U.S. Attorney's Office and the San Diego County District Attorney's Office. Throughout my tenure with HSI, I have participated in numerous investigations involving child exploitation, human trafficking, human smuggling, financial crimes and narcotics. As an HSI Special Agent assigned to the ICAC task force, I investigate criminal violations relating to child exploitation, child pornography and cybercrimes, including violations pertaining to impersonating an officer, in violation of Title 18, United States Code, Section 912, blackmail, in violation of Title 18, United States Code, Section 873, extortion through interstate communications, in violation of Title 18, United States Code, Section 875, mailing threatening communications, in

1 violation of Title 18, United States Code, Section 876, receiving proceeds of
2 extortion, in violation of Title 18, United States Code, Section 880 and conspiracy
3 to commit these offenses, in violation of Title 18, United States Code, Section
4 371. As a federal agent, I am authorized to investigate violations of laws of the
5 United States, and I am a law enforcement officer with the authority to execute
6 warrants issued under the authority of the United States. In preparing this
7 affidavit, I have discussed the facts of this case with other law enforcement agents,
8 including officers within HSI and the Office of Professional Responsibility (OPR).

9
10 2. This affidavit is made in support of an application for a warrant to search for
11 and seize evidence related to potential violations of Title 18, United States Code,
12 Sections 912, 873, 875, 876, 880 and 371, at the location described in Attachment
13 A, for evidence described in Attachment B.

14
15 3. This affidavit is based upon information I have gained through training and
16 experience, as well as upon information relayed to me by other individuals,
17 including law enforcement officers. Since this affidavit is being submitted for the
18 limited purpose of securing a search warrant, I have not included each and every
19 fact known to me concerning this investigation but have set forth only the facts
20 that I believe are necessary to establish probable cause to believe that evidence
21 relating to potential violations of Title 18, United States Code, Sections 912, 873,
22 875, 876, 880 and 371, described in Attachment B, is located at Attachments A.

23
24
25 4. Based upon the following information, I believe there is probable cause to
26 believe that currently located within Attachment A, there is evidence concerning
27 potential violations of Title 18 U.S.C. Sections 912, 873, 875, 876, 880 and 371,
28 more particularly described in Attachment B.
29

BACKGROUND ON FACEBOOK

5. Facebook is a corporation that provides an online social networking service and is headquartered in Menlo Park, California. After registering to use the site, users can create a profile, add others users as “friends,” exchange messages, post status updates and photos, share videos, use various apps and receive notifications when other update their profiles. Facebook has different settings, which allow the users to make certain information publicly-accessible, while keeping other information accessible solely to friends.

INVESTIGATIVE RESULTS

6. On or about August 17, 2015, the Joint Intake Center (JIC) received a complaint from an individual (hereafter referred to as V1). V1 stated he was contacted by an agent from HSI’s Cyber Crime Center (C3)¹ in order to extort money from him. V1 stated the agent identified himself as “Charles ROBERTS” and demanded five hundred dollars (\$500) in order to mitigate a pending arrest warrant for V1. (Agents have searched but have found no individual named “Charles Roberts” listed within the agency HSI or C3, as an agent.) V1 sent \$500 per ROBERTS’ instructions via MoneyGram Reference Number 99283061. V1

¹ The Cyber Crimes Center (C3) is a legitimate section under HSI. It is comprised of the Cyber Crimes Unit, Child Exploitation Investigations Unit, and Computer Forensics Unit. HSI’s C3 delivers computer-based technical services to support domestic and international investigations into cross border crimes and provides training to federal state, local and international law enforcement agencies.

1 said ROBERTS used the email address **c3childexploitaiondivision@gmail.com**
2 [sic] and phone number (407) 731-7186.

3
4 7. On November 24, 2015, SSA James Grundy with HSI's Office of
5 Professional Responsibility and I interviewed V1. V1 stated that during the month
6 of July or August, 2015, he corresponded over email with a person that he
7 believed to be an adult female. He met this person through Craigslist, a classified
8 advertisements website, which includes personals.

9
10 8. V1 stated that approximately two (2) days after his communications with
11 this woman he received a call from "911." When V1 answered, a male identified
12 himself as "Charles ROBERTS," an agent assigned to the "C3 Child Exploitation
13 Division" in Florida. ROBERTS accused V1 of soliciting a minor on Craigslist
14 and viewing a photo of the alleged minor. ROBERTS claimed that he had an
15 arrest warrant for V1 as a result of this violation. ROBERTS then detailed
16 specifics about V1's employment. (V1 later deduced that ROBERTS likely gained
17 knowledge of his employment by querying V1's phone number, which is linked to
18 V1's professional profile on the website LinkedIn.) V1 never saw the original
19 warrant.
20
21

22
23 9. ROBERTS told V1 that according to the C3 investigation, V1 had not had
24 prior violations. ROBERTS said as a result, he spoke with a C3 supervisor who
25 agreed to allow the warrant to be cleared if V1 promptly paid a five hundred dollar
26 (\$500) fine. ROBERTS emailed a copy of a "Warrant Purge" document to V1
27 reflecting what would be filed to nullify the warrant as long as the fine was paid.
28 V1 recalled ROBERTS used a Gmail account with the words "c3" and "child
29

1 exploitation" in the address. V1 stated the "Warrant Purge" displayed the DHS
2 seal, a judge's name, legal jargon related to child exploitation and represented
3 ROBERTS as an officer from the "C3."

4
5 10. ROBERTS directed V1 to a nearby Walmart and told V1 to use
6 MoneyGram to send the funds, since MoneyGram was backed by the federal
7 government and equipped to send ROBERTS a secure payment. V1 completed the
8 money transfer per ROBERTS' instruction. V1 stated after he paid the fine, he
9 then took a closer look at the "Warrant Purge" and realized there were spelling
10 errors in the document and that it probably was a fake. V1 stated ROBERTS again
11 tried to contact him to pay additional fines. V1 subsequently made the report of
12 the extortion.
13

14
15 11. On November 24, 2015, V1 provided SSA Grundy and me a copy of an
16 email he received from ROBERTS on Saturday, August 1, 2015, at 10:47 a.m.
17 Pacific Standard Time (PST). ROBERTS used the email address
18 **c3childexploitaiondivision@gmail.com** [sic] to send a document that V1
19 interpreted as a copy of a warrant. The document has the words "Warrant Purge"
20 and reflects a payment of \$500. The "Warrant Purge" contains the DHS seal with
21 the heading "IN THE DISTRICT COURT OF JUSTICE OF THE STATE OF
22 California FIFTH DISTRICT." Within the body of the document, the investigating
23 agent is identified as "detective CHARLES ROBERTS EMPLOYED AND
24 SWORN IN UNDER THE C3 CHILD EXPLOITATION UNIT."
25

26
27 12. On December 11, 2015, I submitted a DHS Summons to Google, Inc.,
28 requesting all information associated to **c3childexploitaiondivision@gmail.com**.
29

1 The summons was accompanied by a court order commanding Google not to
2 disclose the existence of the DHS Summons. *See* 15MC1444.

3
4 13. On or about December 15, 2015, Google responded to the DHS Summons
5 and provided one file pertaining to the Google account-holder identified as
6 **c3childexploitaiondivision@gmail.com**, with internal Reference Number
7 651819. The following information was provided by Google:

8 Name: Charles Roberts

9 e-Mail: **c3childexploitaiondivision@gmail.com**

10 Services: Gmail, Google Talk, Web History

11 Created on: 2015/07/26-20:50:56-UTC

12 Terms of Service IP: 64.45.224.30, on 2015/07/26-20:50:56-UTC

13 Google Account ID: 482292487891

14 Service remained ongoing through at least through December 15, 2015.

15
16 14. On February 16, 2016, SSA Grundy and I interviewed an additional victim
17 (hereafter referred to as V2). V2 stated that he had been on the personals section
18 of Craigslist in July or August 2015. V2 gave an account similar to V1 about how
19 he initially began communicating with a person he believed to be an adult female.
20 He was then contacted by ROBERTS. ROBERTS identified himself as an agent
21 with HSI's C3 and accused V2 of soliciting a minor.

22
23 15. V2 confirmed he had also spoken with ROBERTS on phone number (407)
24 731-7186 during the month of July/August 2015. V2 stated that ROBERTS has
25 changed his phone number several times since their initial phone conversation.
26 V2 said he had spoken to ROBERTS about thirty (30) minutes before meeting
27 with SSA Grundy and me on February 16, 2016. At that time, ROBERTS was
28
29

1 using the phone number (407) 613-9452. ROBERTS continued to identify himself
2 as a Special Agent with Homeland Security and wanted to be apprised if any other
3 Federal Law Enforcement Agencies were to ever speak with V2 concerning his
4 (ROBERTS') investigation.
5

6 16. During the interview, V2 provided SSA Grundy and me with an email that
7 he received from ROBERTS on August 22, 2015, at 8:40 a.m. PST. The email
8 also contained a document titled "Warrant Purge." The document is similar to the
9 previously-described "Warrant Purge" document sent to V1, although this Warrant
10 Purge contains V2's name and it was sent to V2 under the email address
11 **cybercrimescenter3@gmail.com**.
12

13
14 17. V2 stated he also sent monetary payments in the form of Homeland Security
15 "fees" and "fines" via MoneyGram to ROBERTS at his request. Summons results
16 from MoneyGram confirm multiple transactions sent by V2 to ROBERTS and
17 picked up at a Wal-Mart in Kissimmee, Florida. Open records checks reflect the
18 area code (407) used by the two (2) before mentioned phone numbers utilized by
19 ROBERTS are based principally on Orlando, Florida, but also including all of
20 Orange, Osceola, and Seminole counties. Kissimmee is a city is located in
21 Osceola County, Florida.
22

23
24 18. On one specific occasion, V2 sent \$600 using reference number 98041315
25 to ROBERTS on August 24, 2015. MoneyGram summons results reflected that a
26 man who gave the last name ROBERTS picked up the funds from a Wal-Mart
27 located in Kissimmee, FL on August 25, 2015. On August 26, 2015, an individual
28 identified as Ronnie MONTGOMERY posted a self-produced video to **Facebook**
29

1 **account profile [https://facebook.com/profile.php?id= 100008589613118](https://facebook.com/profile.php?id=100008589613118)** of him
2 picking up \$600 at a Walmart in-store MoneyCenter. MONTGOMERY speaks
3 throughout the video and his voice can be distinctly heard.
4

5 19. On February 18, 2016, V1 and V2 both identified MONTGOMERY's voice
6 played from the video posted to **Facebook account profile**
7 **[https://facebook.com/profile.php?id= 100008589613118](https://facebook.com/profile.php?id=100008589613118)** as the individual they
8 spoke with over the phone known to them as ROBERTS, posing as a DHS agent.
9

10 20. On March 3, 2016, United States Magistrate Judge Karen Crawford of the
11 Southern District of California signed federal search warrants for **Facebook**
12 **account profile [https://facebook.com/profile.php?id= 100008589613118](https://facebook.com/profile.php?id=100008589613118)**. See
13 16MJ0621. The requested results spanned from July 1, 2015 to March 2, 2016.
14
15

16 21. On or about March 17, 2016, I received search warrant results from
17 Facebook regarding **Facebook account profile**
18 **[https://facebook.com/profile.php?id= 100008589613118](https://facebook.com/profile.php?id=100008589613118)**. Contained in the
19 search warrant results were messages sent by MONTGOMERY to other
20 individuals concerning his involvement in criminal activity. Specifically,
21 MONTGOMERY had the following conversation with another individual
22 identified as WR on January 23, 2016:
23
24

25 MONTGOMERY: Yeah I got another lick¹ I be doing works real good I'm
26 in Poinciana now

27 WR: What kinda lick

28
29 ¹ The term "lick" is slang for stealing from someone

1 MONTGOMERY: Cyber crime center

2
3 WR: Wtf is that

4 MONTGOMERY: Some crazy shut brother I make 3500 a week minimum
5 This exchange was not publicly-available. I was only able to retrieve it owing to
6 the previously-identified search warrant.
7

8
9 22. On April 19, 2016, SSA Grundy and I witnessed V2 make a consensual
10 monitored call to ROBERTS. V2 discussed with ROBERTS details about an
11 upcoming payment and emotional difficulties he was having with his family due to
12 the large financial pay-outs required by ROBERTS. During the conversation,
13 ROBERTS handed the phone to a different individual who, in turn, identified
14 himself as a psychologist employed with the Department of Homeland Security.
15

16
17 23. The individual posing as the DHS psychologist directed V2 to tell his family
18 that he had a child overseas and the payments he had been making over the past
19 year were in support of this estranged family he created. V2 inquired what he
20 should do if members of his family were to ask for pictures as proof. ROBERTS
21 subsequently took the phone back from the alleged psychologist and told V2 that
22 he would get V2 pictures of a woman and her child.
23

24
25 24. On April 19, 2016, at approximately 1700 hours PST, V2 received pictures
26 of a female and a toddler from ROBERTS. On or about this date and time,
27 MONTGOMERY posted a link to a video of the same toddler and female to
28 **Facebook account profile** <https://facebook.com/profile.php?id=>
29

1 **100008589613118.** In addition to the video, MONTGOMERY posted the
2 comment "It's a work thing don't ask."

3
4 **PRIOR ATTEMPTS TO OBTAIN DATA**
5

6
7 25. I have made no attempts to obtain the data currently requested. On March
8 3, 2016, I obtained a search warrant for Facebook account profile
9 <https://facebook.com/profile.php?id=100008589613118>. The search warrant
10 results provided by Facebook were up to March 2, 2016, the date in which the
11 warrant was signed. Recent activity in April 2016 indicates that MONTGOMERY
12 continues to use Facebook in furtherance of his criminal activity and as a means in
13 which to communicate with other individuals.
14

15 **GENUINE RISKS OF DESTRUCTION**
16

17
18 26. Based upon my experience and training, and the experience and training of
19 other agents with whom I have communicated, electronically stored data can be
20 permanently deleted or modified by users possessing basic computer skills. In this
21 case, a preservation letter was sent to Facebook on or about February 24, 2016
22 ordering the preservation of data associated with the **Facebook user ID**
23 **<https://facebook.com/profile.php?id=100008589613118>**.
24

25 //

26 //

27 //

28 //

SOCIAL NETWORKING SERVICE

27. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

28. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

29. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which

1 highlights information about the user's "Friends," such as profile changes,
2 upcoming events, and birthdays.

3
4 30. Facebook users can select different levels of privacy for the
5 communications and information associated with their Facebook accounts. By
6 adjusting these privacy settings, a Facebook user can make information available
7 only to himself or herself, to particular Facebook users, or to anyone with access
8 to the Internet, including people who are not Facebook users. A Facebook user
9 can also create "lists" of Facebook friends to facilitate the application of these
10 privacy settings. Facebook accounts also include other account settings that users
11 can adjust to control, for example, the types of notifications they receive from
12 Facebook.
13

14
15 31. Facebook users can create profiles that include photographs, lists of
16 personal interests, and other information. Facebook users can also post "status"
17 updates about their whereabouts and actions, as well as links to videos,
18 photographs, articles, and other items available elsewhere on the Internet.
19 Facebook users can also post information about upcoming "events," such as social
20 occasions, by listing the event's time, location, host, and guest list. In addition,
21 Facebook users can "check in" to particular locations or add their geographic
22 locations to their Facebook posts, thereby revealing their geographic locations at
23 particular dates and times. A particular user's profile page also includes a "Wall,"
24 which is a space where the user and his or her "Friends" can post messages,
25 attachments, and links that will typically be visible to anyone who can view the
26 user's profile.
27
28
29

1 32. Facebook allows users to upload photos and videos, which may include any
2 metadata such as location that the user transmitted when s/he uploaded the photo
3 or video. It also provides users the ability to “tag” (i.e., label) other Facebook
4 users in a photo or video. When a user is tagged in a photo or video, he or she
5 receives a notification of the tag and a link to see the photo or video. For
6 Facebook’s purposes, the photos and videos associated with a user’s account will
7 include all photos and videos uploaded by that user that have not been deleted, as
8 well as all photos and videos uploaded by any user that have that user tagged in
9 them.
10

11
12 33. Facebook users can exchange private messages on Facebook with other
13 users. These messages, which are similar to e-mail messages, are sent to the
14 recipient’s “Inbox” on Facebook, which also stores copies of messages sent by the
15 recipient, as well as other information. Facebook users can also post comments on
16 the Facebook profiles of other users or on their own profiles; such comments are
17 typically associated with a specific posting or item on the profile. In addition,
18 Facebook has a Chat feature that allows users to send and receive instant messages
19 through Facebook. These chat communications are stored in the chat history for
20 the account. Facebook also has a Video Calling feature, and although Facebook
21 does not record the calls themselves, it does keep records of the date of each call.
22
23

24 34. If a Facebook user does not want to interact with another user on Facebook,
25 the first user can “block” the second user from seeing his or her account.
26

27 35. Facebook has a “like” feature that allows users to give positive feedback or
28 connect to particular pages. Facebook users can “like” Facebook posts or updates,
29

1 as well as webpages or content on third-party (*i.e.*, non-Facebook) websites.
2 Facebook users can also become “fans” of particular Facebook pages.
3

4 35. Facebook has a search function that enables its users to search Facebook for
5 keywords, usernames, or pages, among other things.
6

7 36. Each Facebook account has an activity log, which is a list of the user’s posts
8 and other Facebook activities from the inception of the account to the present.
9 The activity log includes stories and photos that the user has been tagged in, as
10 well as connections made through the account, such as “liking” a Facebook page
11 or adding someone as a friend. The activity log is visible to the user but cannot be
12 viewed by people who visit the user’s Facebook page.
13
14

15 37. Facebook Notes is a blogging feature available to Facebook users, and it
16 enables users to write and post notes or personal web logs (“blogs”), or to import
17 their blogs from other services, such as Xanga, LiveJournal, and Blogger.
18
19

20 38. The Facebook Gifts feature allows users to send virtual “gifts” to their
21 friends that appear as icons on the recipient’s profile page. Gifts cost money to
22 purchase, and a personalized message can be attached to each gift. Facebook
23 users can also send each other “pokes,” which are free and simply result in a
24 notification to the recipient that he or she has been “poked” by the sender.
25

26 39. Facebook also has a Marketplace feature, which allows users to post free
27 classified ads. Users can post items for sale, housing, jobs, and other items on the
28 Marketplace.
29

1
2 40. In addition to the applications described above, Facebook also provides its
3 users with access to thousands of other applications (“apps”) on the Facebook
4 platform. When a Facebook user accesses or uses one of these applications, an
5 update about that the user’s access or use of that application may appear on the
6 user’s profile page.

7
8 41. Facebook uses the term “Neoprint” to describe an expanded view of a given
9 user profile. The “Neoprint” for a given user can include the following
10 information from the user’s profile: profile contact information; News Feed
11 information; status updates; links to videos, photographs, articles, and other items;
12 Notes; Wall postings; friend lists, including the friends’ Facebook user
13 identification numbers; groups and networks of which the user is a member,
14 including the groups’ Facebook group identification numbers; future and past
15 event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and
16 information about the user’s access and use of Facebook applications.
17

18
19 42. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP
20 address. These logs may contain information about the actions taken by the user
21 ID or IP address on Facebook, including information about the type of action, the
22 date and time of the action, and the user ID and IP address associated with the
23 action. For example, if a user views a Facebook profile, that user’s IP log would
24 reflect the fact that the user viewed the profile, and would show when and from
25 what IP address the user did so.
26
27
28
29

43. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

44. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By

1 determining the physical location associated with the logged IP addresses,
2 investigators can understand the chronological and geographic context of the
3 account access and use relating to the crime under investigation. Such information
4 allows investigators to understand the geographic and chronological context of
5 Facebook access, use, and events relating to the crime under investigation.
6 Additionally, Facebook builds geo-location into some of its services. Geo-
7 location allows, for example, users to “tag” their location in posts and Facebook
8 “friends” to locate each other. This geographic and timeline information may tend
9 to either inculcate or exculpate the Facebook account owner. Last, Facebook
10 account activity may provide relevant insight into the Facebook account owner’s
11 state of mind as it relates to the offense under investigation. For example,
12 information on the Facebook account may indicate the owner’s motive and intent
13 to commit a crime (e.g., information indicating a plan to commit a crime), or
14 consciousness of guilt (e.g., deleting account information in an effort to conceal
15 evidence from law enforcement).
16

17
18 45. Therefore, Facebook computers are likely to contain all the material
19 described above, including stored electronic communications and information
20 concerning subscribers and their use of Facebook, such as account access
21 information, transaction information, and other account information.
22

23 24 **PROCEDURES FOR ELECTRONICALLY STORED INFORMATION**

25
26 46. Federal agents and investigative support personnel are trained and
27 experienced in identifying communications relevant to the crimes under
28 investigation. The personnel of Facebook are not. It would be inappropriate and
29

1 impractical for federal agents to search the vast computer network of Facebook for
2 the relevant accounts and then to analyze the contents of those accounts on the
3 premises of Facebook. The impact on Facebook's business would be severe.

4
5 47. I anticipate executing this warrant under the Electronic Communications
6 Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A),
7 by using the warrant to require Facebook to disclose to the government copies of
8 the records and other information (including the content of communications)
9 particularly described in Section II of Attachment B. Upon receipt of the
10 information described in Section II of Attachment B, government-authorized
11 persons will review that information to locate the items described in Section III of
12 Attachment B.
13

14
15 48. Based on the foregoing, searching the recovered data for the information
16 subject to seizure pursuant to this warrant may require a range of data analysis
17 techniques and may take weeks or even months. Keywords need to be modified
18 continuously based upon the results obtained. The personnel conducting the
19 segregation and extraction of data will complete the analysis and provide the data
20 authorized by this warrant to the investigating team within ninety (90) days of
21 receipt of the data from the service provider, absent further application to this
22 court.
23

24
25 49. Based upon my experience and training, and the experience and training of
26 other agents with whom I have communicated, it is necessary to review and seize
27 all electronic communications that identify any users of the subject account(s) and
28
29

1 any electronic mails sent or received in temporal proximity to incriminating
2 electronic mails that provide context to the incriminating mails.

3
4 50. All forensic analysis of the imaged data will employ search protocols
5 directed exclusively to the identification, segregation and extraction of data within
6 the scope of this warrant.


7
8 **REQUEST FOR SEALING AND PRECLUSION OF NOTICE**
9

10
11 51. This is an ongoing investigation of which the target is unaware. It is very
12 likely, based upon the above, that evidence of the crimes under investigation exists
13 on computers subject to the control of the targets. There is reason to believe,
14 based on the above, that premature disclosure of the existence of the warrant will
15 result in destruction or tampering with that evidence and seriously jeopardize the
16 success of the investigation. Accordingly, it is requested that this warrant and its
17 related materials be sealed until further order of the Court. In addition, pursuant to
18 Title 18, United States Code, Section 2705(b), it is requested that this Court order
19 the electronic service provider to whom this warrant is directed not to notify
20 anyone of the existence of this warrant, other than its personnel essential to
21 compliance with the execution of this warrant until further order of the Court.
22

23
24 **CONCLUSION**
25

26 52. In conclusion, based upon the information contained in this affidavit, I have
27 reason to believe that evidence, fruits and instrumentalities relating to violations
28
29

1 of Title 18, U.S.C. Sections 912, 873, 875, 876, 880 and 371, are located at the
2 location described in Attachment A.

3
4 
5 Stirling Campbell, Special Agent
6 Homeland Security Investigations
7

8 Subscribed and sworn to before me
9 this 22 day of April 2016.
10

11 
12
13 THE HONORABLE BARBARA L. MAJOR
14 UNITED STATES MAGISTRATE JUDGE
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29

ATTACHMENT A

This warrant applies to information associated with the Facebook user ID <https://facebook.com/profile.php?id=100008589613118> that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B**I. Service of Warrant**

The officer executing the warrant shall permit Facebook, as custodian of the computer files described in Section II below, to locate the files relevant to attachment A and copy them onto removable electronic storage media and deliver the same to the officer or agent.

II. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. ("Facebook"), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for the user ID listed in Attachment A for the dates of March 2, 2016 to April 22, 2016:

- a. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- b. All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
- c. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;
- d. All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

- e. All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;
- f. All "check ins" and other location information;
- g. All IP logs, including all records of the IP addresses that logged into the account;
- h. All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
- i. All information about the Facebook pages that the account is or was a "fan" of;
- j. All past and present lists of friends created by the account;
- k. All records of Facebook searches performed by the account;
- l. All information about the user's access and use of Facebook Marketplace;
- m. The types of service utilized by the user;
- n. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- o. All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- p. All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

1 III. Information to be seized by the government

2
3 All information described above in Section II that constitutes fruits, evidence and
4 instrumentalities of violations of Title 18, United States Code, Sections 912, 873,
5 875, 876, 880 and 371 involving Facebook user ID [https://facebook.com/](https://facebook.com/profile.php?id=100008589613118)
6 [profile.php?id=100008589613118](https://facebook.com/profile.php?id=100008589613118) from March 2, 2016 to April 22, 2016,
including information pertaining to the following matters:

- 7 a. Evidence pertaining to the assuming or pretending to be an officer or
8 employee acting under the authority of the United States or any
9 department, agency or officer thereof.
- 10 b. Evidence indicating how and when the Facebook account was
11 accessed or used, to determine the chronological and geographic
12 context of account access, use, and events relating to the crime under
investigation and to the Facebook account owner;
- 13 c. Evidence indicating the Facebook account owner's state of mind as it
14 relates to the crime under investigation;
- 15 d. The identity of the person(s) who created or used the user ID,
16 including records that help reveal the whereabouts of such person(s).
- 17
18
19
20
21
22
23
24
25
26
27
28
29